Claims

1. A security method for the detection and/or control of unauthorized vehicles (10a, 10b, ...) among a large number of authorized vehicles (12a, 12b, ...) within a controlled geographical zone (2), characterized in that all authorized vehicles are equipped with active licenses (60a, 60b, ...) planned to perform a cryptographic action involving a secret cryptographic key (64), and the controlled geographical zone is equipped with automatic control points (20a, 20b, ...), and optionally with manual control points (40a, 40b, ...), each automatic control point detecting all vehicles crossing a specific road section (21) in its vicinity, and each manual control point selecting vehicles by the action of an operator, the vehicles detected by the automatic control points and the vehicles selected by the manual control points being hereafter referred to as designated vehicles, both types of control points being planned to acquire the results of said cryptographic actions performed by the active licenses of said designated vehicles, a cryptographic authentication algorithm involving a validation key (74) being further performed upon each acquired said result, both types of control points being further planned to associate said acquired results to said designated vehicles, the designation of the vehicles, the acquiring of said results, and the performing of the cryptographic authentication algorithm upon said acquired results not requiring a substantial change in the motion conditions of the vehicles, in particular their velocity, classifying as unauthorized at least vehicles which have been designated but whose said results either have not been acquired or have not been cryptographically authenticated, an alert message being transmitted to enforcement authorities for each vehicle which has been classified as unauthorized, allowing in such a way for an immediate intervention and a possible interception of the unauthorized vehicles, at least some of the control points, hereafter referred to as particular control points, being moreover planned to acquire physical characteristics of said designated vehicles, allowing their direct recognition, said alert message including in this case said physical characteristics.

2. A method as described in claim 1, in which at least some of said active licenses, hereafter referred to as particular active licenses, additionally have distinct identities (62a, 62b, ...), each distinct identity belonging to a group of one or more of said particular active licenses, and distinct identity determination being further performed for all designated vehicles bearing said particular active licenses, upon each said acquired result.

3. A method as described in claim 2, in which said controlled geographical zone contains one or more sub-zones, each vehicle being further authorized or unauthorized for each of the sub-zones, each sub-zone being further equipped with automatic control points and optionally with manual control points, a database

(180) of authorization data regarding said particular active license distinct identities being associated with each sub-zone, each determined distinct identity of a vehicle designated by a control point being further checked against said authorization data in the databases associated with the sub-zones containing that control point, said databases being automatically and/or manually modifiable by the enforcement authorities, additionally classifying as unauthorized vehicles which have been designated but whose said distinct identities are indicated as unauthorized by said authorization data in at least one of the databases associated with the sub-zones containing that control point.

4. A method as described in claim 2, in which data regarding said designated vehicles (such as said particular active licenses distinct identities, control points location, times of designation of vehicles) is additionally recorded, this data being searched for inconsistencies with regard to time and/or vehicles location, the results of this search assisting enforcement authorities in finding potential impersonations of said particular active licenses.

5. A method as described in claim 2, in which said secret cryptographic keys of at least some of said particular active licenses are distinct, each distinct key corresponding to a group of one or more said particular active license distinct identities, this, according to the level of protection required for those said particular active licenses, correspondence between said distinct secret cryptographic keys and said distinct identities being additionally required in order to cryptographically authenticate said results, so that a perpetrator in possession of a particular active license, is prevented from impersonating a particular active license with a different distinct secret cryptographic key.

6. A method as described in claim 1, in which said alert messages are prioritized, according to the control point characteristics, such as its location, alert message history, and/or the time of designation of the vehicle, and/or said acquired physical characteristics if available, and/or current operational intelligence if available, improving the effectiveness of the intervention of the enforcement authorities.

7. A method as described in claim 1, in which drivers of vehicles that are classified as unauthorized, are selectively notified immediately upon the vehicles' classification by means (32) of sending a notification in the control points and means (56) of notification in the vehicle communication units.

8. A method as described in claim 1, in which at least some of the authorized vehicles are additionally provided with removable supports containing at least said secret cryptographic keys.

9. A method as described in claim 1, in which at least some of the authorized vehicles are additionally provided with supports containing at least said secret cryptographic keys, these supports planned to prevent a perpetrator from finding out, through physical penetration and/or deduction, the secret cryptographic keys they contain.

10. A method as described in claim 1, in which at least some of the authorized vehicles are additionally provided with supports containing at least said secret cryptographic keys, these supports being physically attached to said authorized vehicles, in a manner preventing their physical displacement from the vehicles and/or causing their destruction and/or eliminating the said secret cryptographic keys from said supports, in case of an unauthorized displacement attempt.

11. A method as described in claim 1, in which at least some of the authorized vehicles are additionally provided with supports containing at least said secret cryptographic keys, in such a way that all the information produced during said cryptographic action leading to a possible disclosure of said secret cryptographic keys, being exclusively contained in said supports.

12. A method as described in claim 1, in which at least some of said active licenses are additionally associated to PINs (Personal Identification Numbers), said PINs supplied to said active licenses by users in possession of authorized vehicles, said PINs being additionally required by said active licenses in order to generate said results of said cryptographic action, and/or being further required in order to cryptographically authenticate said results.

13. A method as described in claim 1, in which digital elements of a first type are used in performing the cryptographic actions of at least some of said active licenses, said digital elements of the first type being additionally required in order to cryptographically authenticate said acquired results, said digital elements of the first type being furthermore different at different times, preventing in this way the authentication of recorded and replayed said results.

14. A method as described in claim 13, in which said digital elements of the first type are based on the outputs of time clocks.

15. A method as described in claim 13, in which said digital elements of the first type are acquired by the control points and transmitted to said designated vehicles.

16. A method as described in claims 2 and 13, in which said digital elements of the first type are the elements of predefined series associated with distinct identities.

17. A method as described in claim 2, in which digital elements of a second type are generated by at least some of said active licenses, are used in performing the cryptographic actions of these particular active licenses, and are required to be different at different times in order to cryptographically authenticate said results of these particular active licenses, preventing in this way the authentication of recorded and replayed said results.

18. A method as described in claim 1, in which said control points are moreover planned to acquire a credential from the active license of each said designated vehicle, said validation key being securely extracted from each acquired credential by performing a cryptographic extraction algorithm involving an extraction key.

19. A method as described in claim 2, in which said validation key is selected from a list of validation keys, according to said determined distinct identity.

20. A method as described in claim 1, in which the cryptographic process consisting of said cryptographic actions in said active licenses and said cryptographic authentications of said acquired results, is of a symmetric type, an asymmetric type, or a combination of both.

21. A method as described in claim 1, in which at least some of said control points are further planned to associate each said acquired result to a particular designated vehicle.

22. A method as described in claim 1, in which the memory contents of said active licenses can be altered as a consequence of instructions and/or data transmitted from the control points.

23. A method as described in claim 1, in which at least some of said authorized vehicles are additionally provided with second active licenses (60/2a, 60/2b, ...), the first ones (60a, 60b, ...) being hereafter referred to as first active licenses, said second active licenses being planned to perform a second cryptographic action involving a second secret cryptographic key, these authorized vehicles being also provided with removable supports containing at least said second secret cryptographic keys of said second active licenses, at least some of the control points being additionally planned to perform dual interrogation mode, in which these control points further acquire the results of said second cryptographic actions performed by the second active licenses of said designated vehicles,

hereafter referred to as second results, and a second cryptographic authentication algorithm involving a second validation key, being further performed upon each acquired said second result, additionally classifying as unauthorized vehicles which have been designated but whose said second results either have not been acquired or have not been cryptographically authenticated.

24. A method as described in claim 23, in which predetermined correspondences between said first active licenses and said second active licenses are planned, additionally classifying as unauthorized vehicles, which have been designated by a control point in dual interrogation mode, for which said predetermined correspondences have not been verified.

25. A security system for the detection and/or control of unauthorized vehicles (10a, 10b, ...) among a large number of authorized vehicles (12a, 12b, ...) within a controlled geographical zone (2), to implement the method of claim 1, comprising:

- in all authorized vehicles a vehicle communication unit (50), comprising means (52) of activating the transmission of an identification message by the vehicle communication unit, an active license (60) containing a distinct identity (62), and a transmitter (54),
- means of issuing (170), and of revoking (178) of active licenses (60a, 60b),
- at least one database (180) containing authorization data regarding vehicles,
- automatic control points (20a, 20b, ...), and optionally manual control points (40a, 40b, ...), both distributed in the controlled geographical zone (2), each automatic control point comprising means (22) of detection of all vehicles crossing a specific road section (21) in its vicinity, and each manual control point comprising means of selection (42) of vehicles by the action of an operator, the vehicles detected by the automatic control points and the vehicles selected by the manual control points being hereafter referred to as designated vehicles, both types of control points additionally comprising means (24) of activating requests for identification to the vehicle communication units of the designated vehicles, means (26) of reception capable of receiving identification messages transmitted by vehicle communication units, hereafter referred to as vehicle communication unit responses (90a, 90b, ...), and a controller (28) capable of associating vehicle communication unit responses to designated vehicles,
- means (130) of retrieving prior data from the database (180),
- means (140) of classification of designated vehicles,
- at least one operations center (160),
- additional means (44) in the manual control points of notifying the manual control point operator,

- a communication network (100) between at least some of the control points, the database (180), the means of issuing (170) and revoking (178) of active licenses, the means of retrieving prior data (130), the means of classification (140) and the operations centers,

characterized in that:

I) The active license (60) contains in addition a secret cryptographic key (64) associated to the distinct identity (62) of the active license (60), and is planned to perform a cryptographic confirmation algorithm (66) involving at least the distinct identity (62) and the secret cryptographic key (64),

II) The vehicle communication unit response (90) comprises the result of the cryptographic confirmation algorithm (66),

III) Means (70) of cryptographic authentication are planned to check for each vehicle communication unit response (90) whether or not the secret cryptographic key (64) corresponding to the distinct identity (62) contained in the vehicle communication unit response (90) was the one used in the calculation of this response (90), this action involving a validation key (74) corresponding to the same distinct identity (62), and a cryptographic validation algorithm (76),

IV) For every newly authorized vehicle, the means (170) of issuing allocate a distinct identity (62), initialize a new active license (60) to bear the allocated distinct identity (62) and a corresponding secret cryptographic key (64), and update the database (180) with information regarding the newly authorized vehicle (12),

V) The means (178) of revoking are planned to automatically (for example time dependent expiration) and/or manually modify elements in the database (180), particularly those included in a list of distinct identities of active licenses in authorized vehicles' vehicle communication units, hereafter referred to as authorized vehicle list (182), and/or a list of distinct identities of active licenses in unauthorized vehicles' vehicle communication units, hereafter referred to as unauthorized vehicle list (184),

VI) The means of retrieving prior data (130) utilize the distinct identity (62) contained in the vehicle communication unit response (90), in order to retrieve from the database (180), authorization data regarding this vehicle,

VII) The means (140) of classification utilize the data produced by the means (22) of detection, and/or the means (26) of reception, and/or the controller (28), and/or

the means (70) of authentication, and/or the means (130) of retrieving prior data, to determine whether a designated vehicle is authorized or not,

VIII) Means (150) of alert convey to at least one operations center (160) and/or to the means (44) of notifying the manual control point operator, an alert message containing the data provided by the means (26) of reception, and/or the controller (28), and/or the means (70) of authentication, and/or the means (130) of retrieving prior data, for at least some of the vehicles classified as unauthorized,

IX) At least some of the control points comprise in addition means (30) of acquiring physical characteristics of designated vehicles, such as photographic information, plate number, color, vehicle type, weight, the means of alert (150) additionally include said acquired physical characteristics in at least some of the alert messages,

26. A system according to claim 25, in which the means (70) of authentication are additionally planned to determine the validation key (74), by utilizing the distinct identity (62) contained in the vehicle communication unit response (90), to select from a validation key list (80) containing for each distinct identity (62) a corresponding validation key (74), and the means (170) of issuing are also additionally planned to update for every newly authorized vehicle (12) the validation key list (80) with the allocated distinct identity (62) and the corresponding validation key (74).

27. A system according to claim 25, in which the vehicle communication unit response (90) additionally comprises a credential (174), the means (70) of authentication being additionally planned to determine the validation key (74), by utilizing a cryptographic extraction algorithm (86) involving an extraction key (78), in order to securely extract the validation key (74) from the credential (174) contained in the vehicle communication unit response (90), and the means (170) of issuing being also additionally planned to initialize for every newly authorized vehicle (12), the active license (60) with a credential (174) containing the result of a cryptographic binding algorithm (176) involving the validation key (74) and a binding key (172) which corresponds to the extraction key (78).

28. A system according to claim 25, in which the means (24) of activating requests for identification transmit to every designated vehicle an interrogation message.

29. A system according to claim 25, in which the means (24) of activating requests for identification comprise a trigger element in the vicinity of the control

point, that is planned to be detectable by means (52) in the vehicle communication units.

30. A system as described in claim 25, which is utilized to perform additional functions such as Electronic Toll Collection, Access Control, in particular on the perimeter of the controlled geographical zone and/or any of its sub-zones, Vehicle Messaging, Fleet Management, traffic law enforcement, statistical survey, a crime investigation tool.

Noam Kogan _____ Edan Almog _____